



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/721,785	11/22/2000	Cary A. Jardin	042390.P8899	3950

7590 11/29/2005

Crystal D Sayles
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard
7th Floor
Los Angeles, CA 90025

EXAMINER

PICH, PONNOREAY

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 11/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

DETAILED ACTION

The Appeal Brief filed on 9/12/2005 was carefully reviewed by an Appeal Conference. The conferees have considered the applicant's arguments. The conferees agreed with some of the applicant's arguments and withdrew the finality of the Office action dated 1/13/2005.

In view of the Appeal Brief filed on 9/25/2005, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

- (1) file a reply under 37 CFR 1.111 (if this Office action is a non-final) or reply under 37 CFR 1.113 (if this Office action is final); or,
- (2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental Appeal Brief, but no new amendments, affidavits, (37 CFR 1.130, 1.131, or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Claims 1-18 are pending.

Docketing

Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Claim Objections

Claims 1, 4-5, 7-8, 9-12, and 16 are objected to because of the following informalities:

1. Claims 1, 4-5, 7-8, 10-12, and 16 refer to either "the link", "said link", "the first link", or "said first link". The examiner respectfully asks applicant to be consistent with the usage of the words "the" and "said" in the set of claims, especially among a group of claims, i.e. see claims 1 and 4-5.
2. In claim 9, the examiner believes "the" should precede "Internet".
3. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 3-7, 9, and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 3 recites "a secure mode". Claim 1, from which claim 3 depends, also recites "a secure mode". It is unclear if applicant meant for the secure mode recited in claim 3 to be a different secure mode than the one recited in claim 1 or if applicant meant to recite "the secure mode" in claim 3 instead. Clarification is requested.
2. Claims 4-6 recite "the network device" which lacks antecedent basis. The examiner believes applicant may have meant "the network interface device".

Art Unit: 2135

3. Claim 7 recites “the control signal”. Claim 6, from which claim 7 depends, recites “control signals”. It is unclear to which control signal is being referred in claim 7—one of the ones recited in claim 6 or some other control signal. If applicant meant one of the ones recited in claim 6, it is unclear to which control signal among the group of control signals in claim 6 is being referred.
4. As per claim 9, it is unclear how the network being the Internet can cause the non-secured protocol to include HTTP and the secured protocol to include HTTP-S.
5. Claim 11 recites “where said encryption element converts data ... to a secured protocol....” It is unclear how data can be converted to a protocol since a protocol is a standard procedure for doing something. Perhaps applicant meant something more along the lines of converting data using a secure protocol.
6. Any claims not specifically addressed are rejected by virtue of dependency.
7. Appropriate corrections are required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1 and 4 are rejected under 35 U.S.C. 102(b) as being anticipated by McKelvey (US 5,896,499).

Claim 1:

McKelvey discloses the limitations of:

1. A computer (Fig 1, item 100).
2. A network interface device to provide the computer with access to the network (Fig 1, items 175 and 177).
3. A bus monitor, i.e. firewall monitoring program 160, to monitor a first link between the network interface device and the computer, where said monitor reports detected failures or intrusions (col 9, lines 42-53).
4. A security switch, i.e. main processor 110, to switch the first link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor (col 9, lines 46-62).

Claim 4:

McKelvey further discloses wherein said non-secured mode of the first link between the network interface device and the computer uses HTTP protocol (col 9, line 63-col 10, line 5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2135

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2-3, 5, 7-11, 14-15, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over McKelvey (US 5,896,499) in view of applicant's admittance of prior art.

Claim 2:

McKelvey does not explicitly disclose wherein said computer is a server. However, applicant discloses that a computer being a server was well known in the art at the time applicant's invention was made (specification, p1, lines 15-17).

It would have been obvious to one of ordinary skill to incorporate McKelvey's teachings within server computers because McKelvey's teachings would provide security for a computer accessible via a computer network (McKelvey: col 5, lines 35-37), i.e. servers.

Claim 3:

McKelvey does not disclose wherein the network operates in a secured mode using an HTTP-S protocol. However, applicant discloses communication between a network infrastructure and network device using a secure protocol, HTTP-S, was well known in the art at the time applicant's invention was made (specification, p2, lines 13-16).

It would have been obvious to one of ordinary skill to modify McKelvey's invention so that the network operates in a secured mode using an HTTP-S protocol.

Art Unit: 2135

One of ordinary skill would have been motivated to do so because HTTP-S is a standard secure Internet communication protocol.

Claim 5:

McKelvey does not explicitly disclose wherein said secured mode of the first link between the network interface device and the computer uses HTTP-S protocol. However, applicant discloses a network device employing HTTP-S communication protocol as well known in the art at the time applicant's invention was made (specification, p2, lines13-16). Further, in Figure 1 of McKelvey, expansion board uses both secured and non-secured mode of communication. These teachings read on the limitation recited in claim 5.

At the time applicant's invention as made, it would have been obvious to one of ordinary skill in the art to modify McKelvey's invention such that the secured mode of the first link between the network interface device and the computer uses HTTP-S protocol. One of ordinary skill would have been motivated to do so because HTTP-S is a standard secure Internet communication protocol.

Claim 7:

McKelvey does not explicitly disclose an encryption element in the computer, where said encryption element converts data placed on said first link to a secured protocol when the control signal is received from said controller. However, applicant discloses a network device employing HTTP-S communication protocol as well known in the art at the time applicant's invention was made (specification, p2, lines13-16).

Further, in Figure 1 of McKelvey, the expansion board uses both secured and non-secured mode of communication. HTTP-S employs encryption.

It would have been obvious to one of ordinary skill in the art to modify McKelvey's invention such that there was an encryption element in the computer, where said encryption element converts data placed on said first link to a secured protocol when the control signal is received from said controller. One of ordinary skill would have been motivated to do so because it would have allowed for the use of the HTTP-S protocol in McKelvey's computer system. HTTP-S was a standard secure communication protocol at the time applicant's invention was made and McKelvey was interested in utilizing both secure and non-secure communication protocols.

Claim 8:

McKelvey discloses the limitations of:

1. An interface device to provide the computer with access to a network (Fig 1, items 170 and 177).
2. A controller to monitor a link between the interface device and the computer, where said controller switches the link from a non-secured protocol to a secured protocol when failure or intrusions are detected on the link (col 9, lines 46-62).

McKelvey does not explicitly disclose a server. However, applicant discloses that a computer being a server was well known in the art at the time applicant's invention was made (specification, p1, lines 15-17). In light of this, it would have been obvious to one of ordinary skill in the art to modify McKelvey's invention according to the limitation

Art Unit: 2135

recited in claim 8. One of ordinary skill would have been motivated to do so for the same reasons given in claim 2.

Claim 9:

McKelvey further discloses the network is the Internet (Fig 1), such that the non-secured protocol includes HTTP (col 9, line 63-col 10, line 5). McKelvey does not explicitly disclose the secured protocol includes HTTP-S. However, applicant discloses a network device employing HTTP-S communication protocol as well known in the art at the time applicant's invention was made (specification, p2, lines 13-16).

It would have been obvious to one of ordinary skill in the art to modify McKelvey's invention such that the secured protocol includes HTTP-S. One of ordinary skill would have been motivated to do so for the same reasons given in claim 3.

Claim 10:

McKelvey further discloses said controller sends a control signal to the computer when failures or intrusions are detected on the link (col 9, lines 46-62). McKelvey does not explicitly disclose the computer is a server. However, this was obvious to McKelvey's modified invention in light of applicant's admittance of prior art, see claim 8.

Claim 11:

Claim 11 recites a limitation substantially similar to what is recited in claim 7. The difference is claim 7 recites a computer and claim 11 recites a server. A computer being a server is obvious to McKelvey's modified invention in light of applicant's admittance of prior art, see claim 8.

Claim 14 and 18:

McKelvey does not explicitly disclose wherein said secured protocol includes HTTP-S protocol. However, applicant discloses that HTTP-S was a well known secure protocol at the time applicant's invention was made (specification, p2, lines 13-16).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify McKelvey's invention such that when it enters secure mode, it uses HTTP-S protocol for communication. One of ordinary skill would have been motivated to do so because HTTP-S is a standard secure communication protocol.

Claim 15:

Claim 15 recites a limitation similar to what is recited in claim 2 and is rejected for the same reasons.

Claims 6, 12-13, and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over McKelvey (US 5,896,499).

Claim 6:

McKelvey does not explicitly disclose a controller that receives a report from the bus monitor and sends control signals to the network interface device, the security switch, and the computer. However, McKelvey discloses a security switch, i.e. main processor, sends a control signal to disable the embedded security processor depending on the error conditions reported by the bus monitor, i.e. firewall monitoring program (col 9, lines 42-62). The controller reads on a program being executed by the

main processor. A program executing on a processor was standard to computer systems and implicitly disclosed by McKelvey. For the security switch to know to send a control signal to disable the security processor, the controller program must have sent a control signal to the main processor, i.e. to another program executing on the main processor or by setting a flag/register on the processor. When the control signal is sent to disable the security processor, the examiner asserts that it would have been obvious to also send control signals to the network interface device and the computer to inform these components that the operating mode of the computer has changed and to adapt accordingly. One of ordinary skill would have been motivated to send control signals also to the network interface device and the computer to maintain proper system functionality. If the computer and network interface device were to continue operating as if the security processor was still functioning as part of the system, it is very likely that improper system operation would occur.

Claims 12 and 16:

McKelvey discloses the limitation of monitoring a link between a network device and a computer (col 9, lines 42-53). McKelvey discloses first directing the link to use a secured protocol when failures or intrusions are detected on the link (col 9, lines 42-63). Note that operating with a disabled secure processor uses a secured protocol since the secure system resources have been isolated from the compromised or failed security processor.

McKelvey does not explicitly disclose second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected.

Art Unit: 2135

However, the examiner asserts that it was well known and common practice in the art to revert a computer system to its normal operating mode once an error has been fixed or intrusion has been dealt with. It would have been obvious to one of ordinary skill to have modified McKelvey's invention to direct the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected because it is the common thing to do in the art of computing.

Claims 13 and 17:

McKelvey discloses the HTTP protocol (col 9, line 63-col 10, line 5). McKelvey does not explicitly disclose said non-secured protocol includes HTTP protocol. However, HTTP is by definition a non-secured protocol and if the security processor was still active in non-secured mode, HTTP protocol could be used in McKelvey's invention (see Fig 1).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

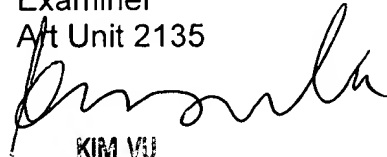
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP

Ponnoreay Pich
Examiner
Art Unit 2135



KIM VU

RECEIVED BY PATENT EXAMINER
TECHNOLOGY CENTER 2135